IN THE CLAIMS:

1. (Currently Amended) A method for defeating, in a server unit of an [IP (]Internet Protocol[)] network, a SYN flooding attack, said server unit running [TCP (Transport] Transmission Control Protocol[)] to allow the establishment of one or more [TCP]transmission control protocol connections with one or more client units, said method comprising the steps of:

upon having activated the transmission control protocol [TCP] in said server unit[:],

listening for the receipt of a SYN message sent from [one said]a client unit;

upon receiving said SYN message[:],

computing an [ISR (]Initial Sequence number Receiver side [)], wherein said Initial Sequence number Receiver side is embedded with connection parameters specified in the SYN message;

responding to said client unit with a SYN-ACK message including said [computed said ISR] Initial Sequence number Receiver side;[:]

resuming to said listening step[.]; and

responsive to receiving an ACK message, determining whether to establish a transmission control block for the client unit by evaluating an incremented value of the Initial Sequence number Receiver side included in the ACK message.

2. (Currently Amended) The method according to claim 1 wherein the step of computing said [ISR] Initial Sequence number Receiver side further includes the steps of:

concatenating a randomly generated key with an identification of one of said [TCP] transmission control protocol connections, [connection] said identification including:

a client socket and a server socket;

a server signature calculated by hashing said concatenation[, thus obtaining a server signature]; and

a concatenation of [concatenating] said server signature and a category index referring to a set of predefined [TCP]transmission control protocol connection categories[;

thereby, obtaining a computed ISR].

3. (Currently Amended) The method according to claim [1 or]2, wherein said computing step further comprises the steps of:

updating, in said server unit, a pseudo-random number (PRN) generator;

holding a current key;

remembering a former key; and

using said current key as said randomly generated key for said [computed ISR] Initial Sequence number Receiver side.

4. (Currently Amended) The method according to claim 2, wherein the step of concatenating said server signature and said category index further includes the [further] step of:

picking [up] a category index within said set of [predefined] connection categories on the basis of [the] content of said [received] SYN message.

5. (Currently Amended) The method according to claim 3, wherein said updating step includes the step of:

updating said PRN generator at a rate not higher than [an MSL (]a Maximum Segment Lifetime[)] defined in said [TCP]transmission control protocol connections [connection].

6. (Cancelled) A method for defeating, in a client unit of an IP network, a SYN flooding attack, said method comprising the steps of:

upon receiving a SYN-ACK message from a server unit:

normally responding with an ACK message, said step of normally responding comprising the step of:

including, in said ACK message, a computed ISR incremented by one.

7. (Currently Amended) A method for defeating, in a server unit of an IP network [having a TCP connection], a SYN flooding attack, said method comprising the steps of:

[upon having activated TCP in said server unit:]

listening for [the receiving of] an ACK message sent from [one] a client unit;

upon receiving said ACK message[:], evaluating

[checking an] a value of an Initial Sequence Number Receiver side that includes content comprising embedded connection parameters specified in a previously received SYN message [ISR;]as an

[if failing said checking step:

dropping said ACK message;

if passing said checking step:

decoding said ISR as being an] authentic computed [ISR] Initial Sequence Number Receiver side; and

responsive to evaluating the value of the Initial Sequence Number Receiver side as an authentic computed Initial Sequence Number Receiver side,

allocating resources for [said TCP] a transmission control protocol connection according to said content [of said computed ISR]; and

[establishing said TCP connection;

in either case:]

resuming said listening step.

8. (Currently Amended) The method of claim 7, further including [wherein the decoding step includes the step of] :

interpreting a category index extracted ~~[[688]]~~ from said [computed] value of the Initial Sequence Number Receiver side [ISR].

9. (Currently Amended) The method according to claim 8, wherein the allocating step includes the step of:

selecting a predefined set of parameters, for said [TCP]transmission control protocol connection, on the basis of the [value of said] category index.

10. (Currently Amended) The method according to claim 7, wherein the step of [checking]evaluating said [ISR]Initial Sequence Number Receiver side includes, upon receiving said ACK message, the steps of:

having, firstly, selected [said]a current key:

getting said [selected]current key;

concatenating said [selected]current key with an identification of said [TCP]transmission control protocol connection, said identification including:

a client socket and a server socket;

hashing said concatenation of the current key and the identification, thus obtaining a re-computed server signature;

extracting an acknowledgment field from said ACK message;

decrementing content of said acknowledgement field;

extracting [said]a server signature from the decremented content; and

comparing said re-computed server signature and said extracted server signature[;].

[if said extracted server signature and said re-computed server signature match:

extracting said category index; if said extracted server signature and said re-computed server signature to not match:

checking if a second loop status is set;

If not set:

selecting a former key [[698]];

setting a second loop status;

resuming execution at said getting step;

if set:

failing said checking step.]

11. (Currently Amended) A computer program product for defeating, in a server unit of an [IP ()]Internet Protocol[)] network , a SYN flooding attack, said server unit running [TCP (Transport] Transmission Control Protocol[)] to allow the establishment of one or more [TCP]transmission control protocol connections with one or more client units, said

computer program product having computer readable program code comprising[the steps of]:

[upon having activated TCP in said server unit:]

computer readable program code, responsive to having activated the transmission control protocol in said server unit, for listening for the receipt of a SYN message sent from [one said]a client unit;

[upon receiving said SYN message:]

computer readable program code for computing an [ISR]Initial Sequence number Receiver side[)] responsive to receiving said SYN message, wherein said Initial Sequence number Receiver side includes embedded connection parameters ;

computer readable program code for responding to said client unit with a SYN-ACK message including said [computed said ISR:]Initial Sequence number Receiver side;

computer readable program code for resuming said listening step; and

computer readable program code for, responsive to receiving an ACK message, determining whether to establish a transmission control block for the client unit by evaluating an incremented value of the Initial Sequence number Receiver side included in the ACK message.

12. (Currently Amended) The computer program product according to claim 11, wherein the [step of] computer readable program code for computing said [ISR]Initial Sequence number Receiver side further includes[the steps of]:

computer readable program code for calculating a concatenation of [concatenating] a randomly generated key with an identification of one of said one or more [TCP connection]transmission control protocol connections, said identification including:

a client socket and a server socket;

[computer readable program code for]a server signature calculated by hashing said concatenation[, thus obtaining a server signature]; and

[computer readable program code for concatenating]a concatenation of said server signature and a category index referring to a set of predefined [TCP]transmission control protocol connection categories[;

thereby, obtaining a computed ISR] .

13. (Currently Amended) The computer program product according to claim 11 or 12 wherein said computing step further comprises the steps of:

computer readable program code means for updating, in said server unit, a pseudo-random number (PRN) generator;

computer readable program code for holding a current key;

computer readable program code for remembering a former key; and

computer readable program code for using said current key as [said randomly generated] the former key for evaluating said [computed ISR]Initial Sequence number Receiver side.

14. (Currently Amended) A system for implementing a shield for defeating TCP SYN flooding attacks, said system comprising:

an [IP (]Internet Protocol[)] network;

a server unit running [TCP (Transportation]Transmission Control Protocol[)] to allow the establishment of one or more [TCP] transmission control protocol connections; and

one or more client units; wherein, once said [TCP]Transmission Control Protocol is activated in said server unit, said server unit listens for the receipt of a SYN message from one or more of said client units[;], and whereupon receiving said SYN message from a client unit, said server unit computes an [ISR (]Initial Sequence number Receiver side [)]having connection parameters embedded therein, responds to said client unit with a SYN-ACK message including said Initial Sequence number Receiver side [computed ISR] and resumes listening for further SYN messages, and wherein said server unit, responsive to receiving an ACK message, determines whether to establish a transmission control block for the client unit by evaluating a value comprising an increment of the Initial Sequence number Receiver side included in the ACK message.